High Technology Investigative Unit Internship Program

DEPARTMENT OF JUSTICE

CHILD EXPLOITATION & OBSCENITY SECTION

Short Term Assignments

Interns will be assigned day-to-day forensic tasks as the need arises. Although it is impossible to predict what these assignments may potentially be, they will often involve discrete short term tasks that can be completed within a day. They may include:

- Date/Time file analysis
- Use i2's Analyst' Notebook to graphically link different suspects.
- Restore hard drives from Encase images.

Assignments will be informal and be delegated according to intern's schedule and availability.

HTIU Committment

The High Technology Investigative Unit (HTIU) is committed to fostering a respectful and productive work environment. Every reasonable precaution will be taken to limit the exposure of interns to criminal and/or contraband materials. It may however, be inevitable that interns be inadvertently exposed, to a limited extent, to some of these materials. Interns are expected to voice their concerns and advise their supervisor of any deleterious effects of these materials immediately.

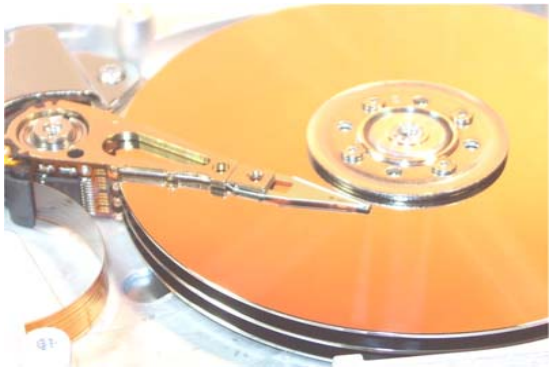
Expectations

While the HTIU recognizes the need for close supervision, interns are expected to handle themselves both professionally and independently. All long term assignments require that interns document their work and turn in a written report at the end of their term.

Additionally, interns are expected to maintain close contact with their academic advisors to ensure that their academic credit requirements are met. Where possible, the HTIU will configure the internship program to meet the needs of the student and their respective school.

HTIU Internship Program

DEPARTMENT OF JUSTICE
CHILD EXPLOITATION & OBSCENITY SECTION



Computer Forensics

Computer forensics is the process of identifying potential evidence on an electronic medium to be used in the court of law. It involves preserving, extracting, documenting and interpreting computer data. Computer forensic specialists use sophisticated tools and software to reconstruct a suspect's movement on the computer. The process goes beyond merely recovering deleted files and require a process and methodology that is forensically sound. Evidence gathered in a criminal investigation must ultimately stand the scrutiny of a potential trial.

About the HTIU

The High Technology Investigative Unit (HTIU) initiates investigations and conducts forensic analysis on computer evidence in federal cases involving child exploitation and obscenity crimes. It works closely with federal agencies such as the FBI, Secret Service, Bureau of Immigration and Customs Enforcement (ICE), and the Postal Inspection Service; as well as federal prosecutors all over the country. The mission of the HTIU is simple: Provide the most accurate, up-to-date expertise on computer forensic matters and assist law enforcement in bringing criminals who peddle in child exploitation and obscenity to justice.

A Unique Opportunity

Your role at the HTIU will be a unique one. The HTIU provides the opportunity for current graduate and undergraduate students to experience the computer forensics field first-hand. You may be asked to restore a Windows PC one day and analyze log files from an electronic wiretap the next. The scope of work is broad, and no day In addition to your short term tasks, you will be asked to complete a long-term assignment that will significantly contribute to the HTIU's overall success.

Long term assignments are based on your particular expertise, career objectives, and the immediate needs of the Unit. You will work with your immediate supervisor to determine you assignment, which may include:
Research and experiment on specific Window's file behaviors to provide conclusive data on the impact of day to day computer usage.
Analyze internet-based software such as AIM, IRC, Newsgroup readers, e-mail clients, etc. to determine the impact of their installation and use on Windows based PC and identify potential points of evidence.
Develop code modules in various programming languages to support ISIS – the HTIU's Internet Site Investigation System.

Now accepting applications for Spring and Summer 2009.

Academic credit and/or paid internships (up to $13.60 per hour) are available.

To apply, send resume by email to HTIU@usdoj.gov

For additional information, contact the HTIU at (202) 514-5780 or by email at HTIU@usdoj.gov

United States citizenship is required

HTIU Internship Program

DEPARTMENT OF JUSTICE
CHILD EXPLOITATION & OBSCENITY SECTION

Hardware	Networking	Software
Build and configure several machines with various versions of Microsoft Windows. Test system file behaviors for each version specifically noting the modification date, creation date, and last accessed date for test files. Test these attributes under the following conditions: •Windows Boot-up process •Automated Virus scanners under different conditions (boot-up, full system scan, e-mail file scan, etc.) •Creation and deletion of .lnk files •Various Windows automated indexing services	Ongoing maintenance of the HTIU network which includes: •Develop and implement a tape back-up process •Maintain user profiles and permissions •Maintain data archives and manage disk usage	Continue development work on ISIS, the HTIU's case investigation system. Based on current skill sets and experience, this may be achieved through one of the following: •Develop mySQL data back-end •Develop Intranet front-end using DreamweaverMX, JAVA or other internet development tool. ** ISIS is developed using a component-based architecture. Interns will work with their supervisor to determine an appropriate component of the system to develop based on their time requirements.*
	Ongoing maintenance and configuration of Red Hat Linux-based Apache Web Server and Samba File Server.	
Build and configure several machines with various versions of Microsoft Windows. Download and configure internet software such as Agent Forte, IRC, Kazaa and Kazaa Lite on each machine and note the effects of each. Identify different areas on the computer that are forensically affected by the install (windows registry, history files, Internet Explorer .dat files, etc.). Further determine what information can be obtained with prolonged usage of each of these programs.		As needed, develop and test automated scripts to perform file analysis functions. This can be achieved with any available scripting and/or programming language. Conduct a feasibility analysis on implementing new and emerging technologies as part of the investigative process. Research newly released tools and software (particularly web capture tools) and test their effectiveness.